

CRISTI

Structuri Algebrice în Informatică

Produsele al polinoamilor

$K = \text{un corp comutativ (e.g. } \mathbb{R}, \mathbb{Q}, \mathbb{C}, \mathbb{Z}_p \text{ sau m)}$

În $\mathbb{R}, \mathbb{Q}, \mathbb{C}$ și $m \neq 0 \wedge m \neq 1 \Rightarrow$ sunt corpuri cu caracteristică zero

$$\mathbb{Z}_p, 1+p=2, \underbrace{1+1+\dots+1}_{p\text{ ori}} = p = 0 \Rightarrow p \cdot 1 = 0, \text{ char}(K) = 0$$

sunt corpuri cu \mathbb{Z}_p este corp de caracteristică p
 $\text{char}(\mathbb{Z}_p) = p$

Def.: Fie $f \in K[x]$. Să suntem că $a \in K$ este rădăcina polinomului f , dacă $f(a) = 0$.

Teorema lui Bézout:

Dati $f \in K[x]$ și $a \in K$, restul împărțirii polinomului f la polinomul $x-a$ este $f(a)$.

* Împreună particular, a este rădăcina pt. $f(x) = 0$

$$\exists g(x) \in K[x] \quad a \cdot 1 \mid f(x) = (x-a)g(x)$$

Dcm: Dăm teorema împărțirii cu rest, $\exists q(x) \in K[x]$,

$$\exists r(x) \in K[x] \quad \text{s.t. } f(x) = (x-a)q(x) + r(x) \quad \text{cu} \\ \text{grad } r(x) < \text{grad } (x-a) = 1 \Rightarrow r(x) \in K$$

$$f(a) = (a-a)q(a) + r(a)$$

restul este $f(a)$

a este rădăcina $\Leftrightarrow f(a) = 0 \wedge f(x) = (x-a)g(x)$ pe
 $u g \in K[x]$

Def: Se presupune că $f \in K[x] \wedge a \in K$ și $f(x) = (x-a)^l g(x)$
 $u g \in K[x], g(a) \neq 0$

Suntem că a este ordinul rădăcinii a în poli-
nomul f .

\hookrightarrow suntem să că a este rădăcina multiplă de
ordinul l pentru f)

Dacă $l=1 \Rightarrow$ suntem că a este rădăcina simplă
pentru f

$$l=2 \rightarrow \text{--} \text{-- dublu} \text{--} \text{--}$$

$$l=3 \rightarrow \text{--} \text{--} \text{--} \text{triplu} \text{--} \text{--} \text{--}$$

$l \geq 2 \rightarrow$ rădăcina multiplă.

Prop: So pp. că $a \in K$: Fie $f \in K[x]$. Astunci
 $a \in K$ este rădăcina pt. f de ordinul (≥ 1).

$\Leftrightarrow f(a) = f'(a) = \dots = f^{(l-1)}(a) \wedge f^{(l)}(a) \neq 0$

Prop: Fie $f \in K[x]$. Dacă $a_1 \in K$ este rădăcina de
ordin l_1 , atunci este $--$ $l_1 \geq 1$

Astunci $\exists g \in K[x]$ a. i. $f(x) = (x-a_1)^{l_1}(x-a_2)^{l_2} \dots (x-a_t)^{l_t} \cdot g(x)$

Astunci $f \in$

mai m. de rădăcini ($\in K$) pt. f este \leq grad f .
(cu tot cu multiplicitate)

$! l_1 + l_2 + \dots + l_t \leq \text{grad } f$

$$\text{Ex: } f(x) = (x-1)(x^2-2) \rightarrow \text{rădăcini } x=1, x_2,3 = \pm\sqrt{2}$$

Teorema lui Viète:

Să presupunem că polinomul $f(x) = a_m x^n + a_{m-1} x^{n-1} + \dots + a_1 x + a_0 \in K[x]$ de grad m ($a_m \neq 0$) are rădăcini $\alpha_1, \alpha_2, \dots, \alpha_m$ (nu neapărat distincte).

$$\begin{aligned} \text{Atunci } f(x) &= a_m (x - \alpha_1)(x - \alpha_2) \dots (x - \alpha_m) = \\ &= a_m x^n - a_m \left(\sum_{i=1}^n \alpha_i \right) x^{n-1} + a_m \left(\sum_{1 \leq i < j \leq m} \alpha_i \alpha_j \right) x^{n-2} + \\ &\quad + \dots + a_m (-1)^n \cdot \prod_{i=1}^n \alpha_i \end{aligned}$$

Identificând coeficientul relativ la x^{n-1} :

$$\sum_{i=1}^n \alpha_i = \frac{a_{m-1}}{a_m}$$

$$\sum_{1 \leq i < j \leq m} \alpha_i \alpha_j = \frac{a_{m-2}}{a_m}$$

$$\prod_{i=1}^n \alpha_i = (-1)^{n-1} \cdot \frac{a_0}{a_m}$$

Divizibilitate, GCD & LCM

Def: $f \in K[x]$ dividi pe polinomul $g \in K[x]$ dacă
 f/g dacă și număr $f \cdot h = g$

Relația „|” pe $K[x]$ este reflexivă
și transzitivă
dar de obicei nu este antireflexivă

Def: Spunem că f_1 și $f_2 \in K[x]$ sunt asociate în
divizibilitate ($f_1 \sim f_2$) dacă $f_1/f_2 \sim f_2/f_1$.

Prop. Fie $f_1, f_2 \in K[x]$. Astunci $f_1/f_2 \not\sim f_2/f_1$

(\Leftarrow) $\exists \lambda \in K \setminus \{0\}$ a. s. $f_1 = \lambda f_2$

Indec: $f_1 \cdot h_1 = f_2 \Rightarrow h_1 \cdot h_2 \cdot f_2 = f_2 \Rightarrow (f_2)(1 - h_1 \cdot h_2) = 0$
 $\Rightarrow f_2 = 0 \Rightarrow f_1 = 0$ $\begin{matrix} f_1 = h_2 \cdot f_2 \\ \uparrow \qquad \downarrow \end{matrix} \quad \begin{matrix} h_1 \cdot h_2 = 1 \\ \text{K}[x] \qquad \text{grad } 0 \end{matrix} \quad \Rightarrow h_1, h_2 \in K \setminus \{0\}$

$\text{grad } h_1 + \text{grad } h_2 = 0$

$d = \text{GCD}(f_1, f_2)$

GCD

Def. Fie $f_1, f_2 \in K[x]$. Spunem că $d \in K[x]$ este
un cel mai mare div. comun pt. f_1, f_2 dacă

(1) $d | f_1 \wedge d | f_2$

(2) $\forall h \in K[x]$ cu $h | f_1 \wedge h | f_2 \Rightarrow h | d$.

Analog pt LCM (f_1, f_2)

În $K[x]$ GCD-ul este unic pînă la o asociere
în divizibilitate

α multe ori preferă să alegem $\gcd(f_1, f_2)$ nu
pe polinom monic.

Dif: $f_1, f_2 \in K[x]$ oprimă co-mulți prime între
ele dacă $\gcd(f_1, f_2) = 1$ (=) = orice constanță
natură.

Teorema (Euclid): Pentru orice $f_1, f_2 \in K[x]$ există
 $\gcd(f_1, f_2) \in K[x]$ și $u(x), v(x) \in K[x]$
a.s.t. $u \cdot f_1 + v \cdot f_2 = \gcd(f_1, f_2)$

Dem: Alg lui Euclid

\rightarrow facem împărțirea rest neroare cond gradim $r=0$
iar $\gcd(f_1, f_2)$ = ultimul rest nenul
 $f_1 = q_1 \cdot f_2 + r_1$ cu grad $r_1 < \text{grad } f_2$
 $f_2 = q_2 \cdot r_1 + r_2$ cu grad $r_2 < \text{grad } r_1$

Prop: dacă f_1, g sunt prime între ele \Rightarrow

$\Rightarrow f \mid h$

temo: $\gcd(x^a - 1, x^b - 1) = ?$

Polinoame ireductibile

Dif: Un polinom neconstant din $K[x]$ și număr
ireductibil în $K[x]$ dacă nu se poate scrie ca
produs de polinoame neconstante.

$f = f_1 \cdot f_2$ în $K[x] \Rightarrow f_1 \in K$ sau $f_2 \in K$,
cu grad $f \geq 1$

Dacă f este un polinom neronsonant cu nu e redusabil în $K[x]$, o punemă f este redusabil în $K[x]$.

Propozitie: Fie $f \in K[x]$

a) dacă $\text{grad } f = 1 \Rightarrow f$ este redusabil în $K[x]$.

b) dacă f este inductibil în $K[x]$, și $\text{grad } f \geq 2$, atunci f nu are rădăcini în K.

c) dacă $\text{grad } f \in \{2, 3\}$, atunci f este redusabil în $K[x]^\ominus$ f nu are rădăcini în K.

Ex: $x^2 - 2 \in \mathbb{Q}[x]$ are rădăcini $\pm\sqrt{2} \in \mathbb{R} \setminus \mathbb{Q}$ deci este inductibil în $\mathbb{Q}[x]$, deci redusabil în $\mathbb{R}[x]$

$$x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$$

$$\in \mathbb{R}[x] \not\subset \mathbb{Q}[x]$$

Ex: $(x^2 - 1)(x^2 - 3) \in \mathbb{Q}[x]$ este redusabil în $\mathbb{R}[x]$, deci nu are rădăcini în \mathbb{R} , $\pm\sqrt{2} \neq \pm\sqrt{3} \in \mathbb{Q}$

Prop: Fie $f \in K[x]$

f este inductibil în $K[x]^\ominus$ și $g, h \in K[x]$

$$f | gh \Rightarrow f | g \text{ sau } f | h$$

Teorema de descompunere în factori inductibili:

Orică polinom neronsonant din $K[x]$ se descompune ca produs de polinoame inductibile, iar descompunerea sa este unică pînă la o ordene de divizibilitate a factorilor.

$f \in K[x]$ $f = \lambda \cdot p_1^{a_1} \cdot p_2^{a_2} \cdots \cdot p_t^{a_t}$ cu $\lambda \in K \setminus \{0\}$
 grad $f \geq 1$ unde

$p_1, \dots, p_t \in K[x]$ inductibile in $K[x]$, distincte
 $a_i > 0$

Prop. Există în $K[x]$ o infinitate de polinoame inductibile.

Cazul $\mathbb{Q}[x]$

Teorema: Un polynom neconstant din $\mathbb{Q}[x]$ este inductibil (\Leftrightarrow are gradul 1)

$ax+b$, $a, b \in \mathbb{Q}$, $a \neq 0$

Teorema fundamentală a algebrei (D'Alembert-Gauss)

Orice polynom neconstant $f \in \mathbb{Q}[x]$ are cel puțin o rădăcină în \mathbb{Q}

Pf. $f \in \mathbb{Q}[x]$ de grad $n \geq 1$.

$$f(x) = \lambda (x - \alpha_1)^{e_1} (x - \alpha_2)^{e_2} \cdots (x - \alpha_n)^{e_n}$$

cazul $x \in \mathbb{Q}^*$ este dec. în factori ined.

Cazul $\mathbb{R}[x]$

Teorema: Un polynom neconstant și dim $\mathbb{R}[x]$ este inductibil în $\mathbb{R}[x]$.

\Leftrightarrow (grad $f=1$) sau (grad $f=2$ și nu are rădăcini reale)

$ax^2 + bx + c$ și $a \neq 0$, $a, b, c \in \mathbb{R}$

$$\text{și } \Delta = b^2 - 4ac < 0$$

Cazul $\mathbb{Z}_p[x]$: PE $f \in \mathbb{Z}_p[x]$ cu grad $f = m \geq 1$
avem un nr. finit de polinoame
in $\mathbb{Z}_p[x]$ de grad $< m$ si putem
verifica daca dreptul din ele se
divide pt f .
Alg. Berlekamp & (suplimentar)